

WHAT IS CLAIMED IS:

1. A method for performing network address translation on data, the method comprising:

receiving a first data having a first source address and a first
5 destination address, wherein the first data is sent by a first domain source to a
second domain destination, and wherein the first data is received into a first
interface;

obtaining routing information for the first data;

when the first source address is private, translating the first source
10 address into a first public address and forming a first binding between the first
source address, the first public address, and the first interface if there is not
such a binding formed already, wherein the translation is performed prior to
sending the first data to the second domain destination;

when the first destination address has an associated binding,
15 translating the first destination address into a first private address specified by
the binding associated with the first destination address, wherein the
translation of the first destination address is performed prior to sending the
first data to the second domain destination; and

20 sending the first data to the second domain destination based on the
routing information.

2. A method as recited in claim 1, wherein the first binding is formed using one
or more Translation Tables.

3. A method as recited in claim 1, wherein the first public address is selected from a pool of available public addresses.

4. A method as recited in claim 1, wherein when the first data has a DNS payload, the method further comprises:

5 translating the DNS payload of the first data into a second public address, wherein the translation of the first destination address is performed prior to sending the first data to the second domain destination; and

forming a second binding between the DNS payload address, the second public address, and the first interface.

10 5. A method as recited in claim 4, wherein translating the DNS payload and forming a second binding are only performed when the DNS payload contains a private address.

6. A method as recited in claim 1, wherein the first data is a DNS request, the method further comprising:

15 receiving a second data after the first data, wherein the second data has a second source address, a second destination address, and a DNS payload address, wherein the second data is sent by the second domain source to the first domain destination, and wherein the second data is a DNS reply received into a second interface;

20 obtaining routing information for the second data;
when the DNS payload address is private, translating the DNS payload address into a second public address and forming a second binding between the DNS payload address, the second public address, and the second interface,

wherein the translation is performed prior to sending the second data to the first domain destination; and

sending the second data to the first domain destination based on the routing information obtained for the second data.

5 7. A method as recited in claim 6, wherein the first binding between the first source address, the first public address, and the first interface is formed by creating a first entry in a first table that includes a first identifier for both the first public address and the first destination address, a destination pointer that references information on how to translate a destination address of a first subsequently received data from the first public address to the first source address, and a source pointer that references a null value.

8. A method as recited in claim 7, wherein the source pointer referencing a null value indicates that the source address of the first subsequently received data does not require translation.

9. A method as recited in claim 8, the method further comprising modifying the first binding, wherein the first binding is modified and the second binding is formed by:

creating a second entry in the first table that includes a second identifier for both the first source address and the second public address, a destination pointer that references information on how to translate a destination address of a second subsequently received data from the second public address into the DNS payload address, and a source pointer that references information on how to translate a source address of the same second subsequently received data from the first source address into the first public address; and

creating a third entry in the first table that includes a third identifier for both the DNS payload address and the first public address, a destination pointer that references information

on how to translate a destination address of a third subsequently received data from the first public address into the first source address, and a source pointer that references information on how to translate a source address of the third subsequently received data from the DNS payload address into the second public address.

5 10. A method as recited in claim 9, wherein the destination and source pointers each reference a pair having a private address of a particular interface and a corresponding public address, wherein the pair provide pre-translation and post-translation addresses for a particular source or destination address.

10 11. A method as recited in claim 1, further comprising tracking which interfaces may communicate with which other interfaces.

12. A method as recited in claim 11, wherein tracking is accomplished by setting up or dismantling one or more groups that each define which interfaces may communicate with each other.

15 13. A method as recited in claim 12, the method further comprising selecting a pool of public addresses for each group.

14. A network address translation (NAT) system operable to perform network address translation on data, the NAT system comprising:

one or more processors;

one or more memory, wherein at least one of the processors and memory are

20 adapted to:

receive a first data having a first source address and a first destination address, wherein the first data is sent by a first domain source to a second domain destination, and wherein the first data is received into a first interface;
obtain routing information for the first data;

5 when the first source address is private, translate the first source address into a first public address and forming a first binding between the first source address, the first public address, and the first interface if there is not such a binding formed already, wherein the translation is performed prior to sending the first data to the second domain destination;

10 when the first destination address has an associated binding, translate the first destination address into a first private address specified by the binding associated with the first destination address, wherein the translation of the first destination address is performed prior to sending the first data to the second domain destination; and

15 send the first data to the second domain destination based on the routing information.

15. A NAT system as recited in claim 14, wherein when the first data has a DNS payload, one or more memory, wherein at least one of the processors and memory are further adapted to:

20 translate the DNS payload of the first data into a second public address, wherein the translation of the first destination address is performed prior to sending the first data to the second domain destination; and

form a second binding between the DNS payload address, the second public address, and the first interface.

16. A NAT system as recited in claim 15, wherein translating the DNS payload and forming a second binding are only performed when the DNS payload contains a private address.

17. A NAT system as recited in claim 14, wherein the first data is a DNS request,
5 wherein at least one of the processors and memory are further adapted to:

receive a second data after the first data, wherein the second data has a
second source address, a second destination address, and a DNS payload
address, wherein the second data is sent by the second domain source to the
first domain destination, and wherein the second data is a DNS reply received
10 into a second interface;

obtain routing information for the second data;

when the DNS payload address is private, translate the DNS payload
address into a second public address and forming a second binding between
the DNS payload address, the second public address, and the second interface,
15 wherein the translation is performed prior to sending the second data to the
first domain destination; and

send the second data to the first domain destination based on the
routing information obtained for the second data.

18. A NAT system as recited in claim 17, wherein the first binding between the
20 first source address, the first public address, and the first interface is formed by creating a
first entry in a first table that includes a first identifier for both the first public address and
the first destination address, a destination pointer that references information on how to

translate a destination address of a first subsequently received data from the first public address to the first source address, and a source pointer that references a null value.

19. A NAT system as recited in claim 18, wherein the source pointer referencing a null value indicates that the source address of the first subsequently received data does not
5 require translation.

20. A NAT system as recited in claim 19, wherein at least one of the processors and memory are further adapted to modify the first binding, wherein the first binding is modified and the second binding is formed by:

creating a second entry in the first table that includes a second identifier for both the
10 first source address and the second public address, a destination pointer that references information on how to translate a destination address of a second subsequently received data from the second public address into the DNS payload address, and a source pointer that references information on how to translate a source address of the same second subsequently received data from the first source address into the first public address; and

15 creating a third entry in the first table that includes a third identifier for both the DNS payload address and the first public address, a destination pointer that references information on how to translate a destination address of a third subsequently received data from the first public address into the first source address, and a source pointer that references information on how to translate a source address of the third subsequently received data from the DNS
20 payload address into the second public address.

21. A NAT system as recited in claim 20, wherein the destination and source pointers each reference a pair having a private address of a particular interface and a

corresponding public address, wherein the pair provide pre-translation and post-translation addresses for a particular source or destination address.

22. A NAT system as recited in claim 14, wherein at least one of the processors and memory are further adapted to track which interfaces may communicate with which other interfaces.

23. A NAT system as recited in claim 22, wherein tracking is accomplished by setting up or dismantling one or more groups that each define which interfaces may communicate with each other.

24. A NAT system as recited in claim 23, wherein at least one of the processors and memory are further adapted to select a pool of public addresses for each group.

25. A computer program product for performing network address translation on data, the computer program product comprising:

at least one computer readable medium;

computer program instructions stored within the at least one computer readable product configured to cause a network address translation system to:

receive a first data having a first source address and a first destination address, wherein the first data is sent by a first domain source to a second domain destination, and wherein the first data is received into a first interface;

obtain routing information for the first data;

when the first source address is private, translate the first source address into a first public address and forming a first binding between the first source address, the first public address, and the first interface if there is not

such a binding formed already, wherein the translation is performed prior to sending the first data to the second domain destination;

when the first destination address has an associated binding, translate the first destination address into a first private address specified by the binding associated with the first destination address, wherein the translation of the first destination address is performed prior to sending the first data to the second domain destination; and

send the first data to the second domain destination based on the routing information.

26. A computer program product as recited in claim 25, wherein when the first data has a DNS payload, one or more memory, wherein the computer program instructions are further configured to cause the network address translation system to

translate the DNS payload of the first data into a second public address, wherein the translation of the first destination address is performed prior to sending the first data to the second domain destination; and

form a second binding between the DNS payload address, the second public address, and the first interface.

27. A computer program product as recited in claim 26, wherein translating the DNS payload and forming a second binding are only performed when the DNS payload contains a private address.

28. A computer program product as recited in claim 25, wherein the first data is a DNS request, wherein the computer program instructions are further configured to cause the network address translation system to

receive a second data after the first data, wherein the second data has a second source address, a second destination address, and a DNS payload address, wherein the second data is sent by the second domain source to the first domain destination, and wherein the second data is a DNS reply received into a second interface;

obtain routing information for the second data;

when the DNS payload address is private, translate the DNS payload address into a second public address and forming a second binding between the DNS payload address, the second public address, and the second interface, wherein the translation is performed prior to sending the second data to the first domain destination; and

send the second data to the first domain destination based on the routing information obtained for the second data.

29. A computer program product as recited in claim 28, wherein the first binding between the first source address, the first public address, and the first interface is formed by creating a first entry in a first table that includes a first identifier for both the first public address and the first destination address, a destination pointer that references information on how to translate a destination address of a first subsequently received data from the first public address to the first source address, and a source pointer that references a null value.

30. A computer program product as recited in claim 29, wherein the source pointer referencing a null value indicates that the source address of the first subsequently received data does not require translation.

31. A computer program product as recited in claim 30, wherein the computer program instructions are further configured to cause the network address translation system to modify the first binding, wherein the first binding is modified and the second binding is formed by:

5 creating a second entry in the first table that includes a second identifier for both the first source address and the second public address, a destination pointer that references information on how to translate a destination address of a second subsequently received data from the second public address into the DNS payload address, and a source pointer that references information on how to translate a source address of the same second subsequently
10 received data from the first source address into the first public address; and

 creating a third entry in the first table that includes a third identifier for both the DNS payload address and the first public address, a destination pointer that references information on how to translate a destination address of a third subsequently received data from the first public address into the first source address, and a source pointer that references information
15 on how to translate a source address of the third subsequently received data from the DNS payload address into the second public address.

32. A computer program product as recited in claim 31, wherein the destination and source pointers each reference a pair having a private address of a particular interface and a corresponding public address, wherein the pair provide pre-translation and post-
20 translation addresses for a particular source or destination address.

33. A computer program product as recited in claim 25, wherein the computer program instructions are further configured to cause the network address translation system to track which interfaces may communicate with which other interfaces.

34. A computer program product as recited in claim 33, wherein tracking is accomplished by setting up or dismantling one or more groups that each define which interfaces may communicate with each other.

35. A computer program product as recited in claim 34, wherein the computer
5 program instructions are further configured to cause the network address translation system to select a pool of public addresses for each group.

36. An apparatus for performing network address translation on data, the apparatus comprising:

means for receiving a first data having a first source address and a first destination
10 address, wherein the first data is sent by a first domain source to a second domain destination, and wherein the first data is received into a first interface;

means for obtaining routing information for the first data;

means for translating the first source address into a first public address and forming a
first binding between the first source address, the first public address, and the first interface
15 if there is not such a binding formed already when the first source address is private, wherein the translation is performed prior to sending the first data to the second domain destination;

means for translating the first destination address into a first private address specified
by the binding associated with the first destination address when the first destination address
has an associated binding, wherein the translation of the first destination address is
20 performed prior to sending the first data to the second domain destination; and

means for sending the first data to the second domain destination based on the routing information.

37. A method as recited in claim 36, wherein the first data is a DNS request, the apparatus further comprising:

means for receiving a second data after the first data, wherein the second data has a second source address, a second destination address, and a DNS payload address, wherein the second data is sent by the second domain source to the first domain destination, and wherein the second data is a DNS reply received into a second interface;

means for obtaining routing information for the second data;

means for translating the DNS payload address into a second public address and forming a second binding between the DNS payload address, the second public address, and the second interface when the DNS payload address is private, wherein the translation is performed prior to sending the second data to the first domain destination; and

means for sending the second data to the first domain destination based on the routing information obtained for the second data.